Press Release

United States Secret Service

Department of Homeland Security

December 9, 2020
CMR 14-20

SECRET SERVICE HOSTS CYBER INCIDENT RESPONSE SIMULATION

WASHINGTON - Today the Secret Service hosted a virtual Cyber Incident Response Simulation for financial services, real estate, retail and hospitality executives who trained on mitigation strategies for a simulated business email compromise (BEC) attack. Business Email Compromise is a sophisticated scam targeting both businesses and individuals performing a transfer of funds. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

The training was the fifth of its kind and the third virtual event hosted by the Secret Service and its Cyber Fraud Task Force (CFTF) partners. It offered executives who play an active part within their organization's cyber incident response a simulated scenario to enhance planning, collaboration and information sharing between private organizations and the Secret Service.

"The amount of information stored digitally is staggering and the potential cost of a similar attack on a large corporation could be devastating," said U.S. Secret Service Director Jim Murray to participants of the exercise. "Our ability to effectively respond to cyber incidents, like the one we are modeling in our exercise today, is tied very closely to the strength of our relationships with businesses and organizations just like yours."

As the cyber mission of the Secret Service expands, the agency has adopted a multifaceted approach inclusive of education and information sharing, as well as the enhanced development of partnerships with industry representatives. Event participants worked through a uniquely designed cybercrime crisis role-play simulation in order to gain experience, knowledge, and a better understanding of how to efficiently and effectively respond to a BEC attack.

"Cyber incident response simulations are critical to ensuring we have the skills, technology, infrastructure, and public-private sector relationships to respond should a cyber incident occur," said Secretary of the Treasury Steven T. Mnuchin who joined Director Murray at Secret Service Headquarters. "Treasury continues to work with our interagency, international, and industry partners to strengthen our defenses against malicious cyber incidents, as well as ensure swift response efforts to recover related financial losses."

The event featured guest speakers from across law enforcement as well as industry executives who discussed a range of topics including:

- partnerships between the Secret Service, the Department of Homeland Security Cyber Infrastructure Security Agency (CISA); Mastercard, Hogan Lovells and FinCEN;
- the complex cyber-threat environment;
- the needs of organizations victimized by cybercrime, and;
- the capabilities, investigative processes and tools of the Secret Service, specifically the capabilities of the Cyber Fraud Task Force partners.

To learn more about the Secret Service investigative mission, visit us at: www.secretservice.gov.

For questions concerning this release, please contact the U.S. Secret Service Office of Communication and Media Relations at 202-406-5708.